

How to use Active Directory Discovery

- [Overview](#)
- [How To](#)
- [TechNet Blog](#)

Overview

Active Directory Discovery queries Active Directory for a list of network subnets and discovers each in turn.

NOTE - You will need the ports for WMI on the Windows firewall opened on each target Windows computer. For Windows Core servers, ensure you allow the firewall connections as per the TechNet blog post below.

How To

To use Discovery we require access credentials on the target devices. Go to Discover -> Credentials -> Create Credentials and create credentials for all the types of devices you have. They may be for Windows, SSH (Linux / OSX / etc), SNMP, etc.

Once these have been completed you can go to Discover -> Discoveries -> Create Discoveries.

Open the advanced options by clicking on the "Advanced" button. Change the 'type' attribute to Active Directory, input the Active Directory Domain Controller you would like to query and the name of your domain.

Click the "Submit" button and you will be directed to the Discovery list page.

When you click Execute to start the Discovery, Open-Audit will query the specified Domain Controller for a list of network subnets belonging to the domain. Open-Audit will then create a discovery entry for each subnet (if it doesn't already exist) and commence discovery for that subnet.

And that's it! As always, it's too easy 😊

TechNet Blog

Originally at http://blogs.technet.com/b/brad_rutkowski/archive/2007/10/22/unable-to-remotely-manage-a-server-core-machine-mmc-wmi-device-manager.aspx

Unable to remotely manage a Server Core machine (MMC, WMI, Device Manager)

BooRadely 22 Oct 2007 5:56 PM

I've been seeing a lot of churn internally and externally about installing a role on a server core machine and then trying to connect to it remotely only to find that the remote server core machine won't allow you to connect.

Remote Management

To allow remote management of a server core machine run this locally on the box:

```
C:\>netsh advfirewall set currentprofile settings remotemanagement enable
Ok.
```

After which point the firewall should allow all your remote admin tools to connect (computer management and DNS snap-in for example).

WMI

If you're looking for WMI to be open on your servers:



```
C:\>netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

Updated 4 rule(s).
Ok.
```

Device Manager

You can enable a *read-only* view of device manager remotely by doing the following:

- 1) On the server core machine enable remote management (see above).
- 2) On a full server open gpedit.msc and connect to the server core machine.
- 3) Go to: Computer Configuration\Administrative Templates\System\Device Installation
- 4) Enable the following policy: Allow remote access to the PnP interface.
- 5) Reboot the Server Core machine.
- 6) Now you should be able to access the device manager snap-in remotely from a full server.

 Open-Audit Enterprise 2.0.1 Discover ▾ Report ▾ Manage ▾ Modules ▾ Licenses ▾ Admin ▾ Help ▾  User: admin ▾

[Home](#) / [Discoveries](#)
Discoveries

Discoveries List Discoveries ?

ID

Name

Org ID Default Organisation ▾

Description

Type Active Directory ▾

Devices Assigned to Org ▾

Devices Assigned to Location ▾

Network Address

Active Directory Server

Active Directory Domain

NOTE

Before running an Active Directory discovery, make sure you have stored your Windows credentials in [Credentials](#).

Edited By

Edited Date

Last Run

Complete